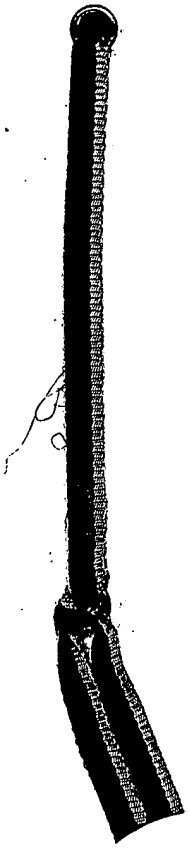
BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung



Aktenzeichen: 101 25 383.4

Anmeldetag: 23. Mai 2001

Anmelder/Inhaber: Siemens Aktiengesellschaft, München/DE

Bezeichnung: Verschlüsselung von Steuerungsprogrammen

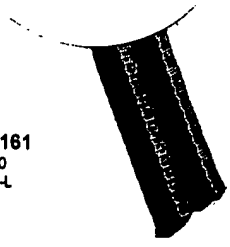
Priorität:
15.12.2000 DE 100 62 741.2
18.12.2000 DE 100 63 059.6
21.12.2000 DE 100 64 400.7

IPC: H 04 L, G 05 B

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 12. November 2001
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Sieck



A 9161
03/00
EDV-L

CERTIFIED COPY OF
PRIORITY DOCUMENT

Beschreibung

Verschlüsselung von Steuerungsprogrammen

Die vorliegende Erfindung betrifft ein Verfahren und eine Vorrichtung zum Transfer von Steuerungsprogrammen und insbesondere ein Verfahren und eine Vorrichtung zur Parametrierung, Projektierung und Inbetriebnahme von Steuerungssystemen und/oder Antrieben mit einem derartigen Verfahren zum Transfer von Steuerungsprogrammen.

Die Steuerungsprogramme von programmierbaren Steuerungen werden in der Regel in so genannten Entwicklungs- oder Engineeringsystemen erstellt. Engineeringsysteme dienen neben dem Erstellen von Steuerungsprogrammen auch zur Inbetriebnahme, Projektierung und Parametrierung von Steuerungen und Antrieben.

Es ist durchaus üblich, dass das Erstellen der Steuerungsprogramme durch ein erstes Fachteam und das Inbetriebnehmen, Projektieren und Parametrieren durch ein zweites Fachteam erfolgt, wobei beide Fachteams örtlich voneinander getrennt sind. Dies bedeutet, dass das vom ersten Fachteam erstellte Steuerungsprogramm zur weiteren Verwendung zu dem zweiten Fachteam übermittelt werden muss. Dabei ist es vielfach wünschenswert, dass zum einen rasche Übertragungswege genutzt werden können und zum anderen bei der Übermittlung eine gewisse Vertraulichkeit gewahrt wird, damit das jeweilige Know-how nicht beliebig zugänglich ist.

Somit besteht die Aufgabe der vorliegenden Erfindung darin, ein Verfahren und ein System vorzuschlagen, mit denen ein geschützter und rascher Transfer von Steuerungsprogrammen ermöglicht wird.

Erfindungsgemäß wird diese Aufgabe gelöst durch ein Verfahren zum Transfer von Steuerungsprogrammen durch Verschlüsseln ei-

nes Steuerungsprogrammcodes in einem ersten Entwicklungssystem, Transferieren des verschlüsselten Steuerungsprogrammcodes von dem ersten Entwicklungssystem zu einem zweiten Entwicklungssystem und Entschlüsseln des verschlüsselten Steuerungsprogrammcodes in dem zweiten Entwicklungssystem.

Darüber hinaus wird die genannte Aufgabe gelöst durch ein System zum Transfer von Steuerungsprogrammen mit einer ersten Entwicklungseinrichtung zum Entwickeln eines Steuerungsprogrammcodes, die eine Verschlüsselungseinheit zum Verschlüsseln des Steuerungsprogrammcodes umfasst, einer Kommunikationseinrichtung zum Transferieren des verschlüsselten Steuerungsprogrammcodes von der ersten Entwicklungseinrichtung zu einer zweiten Entwicklungseinrichtung und der zweiten Entwicklungseinrichtung, die eine Entschlüsselungseinrichtung zum Entschlüsseln des verschlüsselten Steuerungsprogrammcodes umfasst. In vorteilhafter Weise ermöglicht die Erfindung somit, das den Steuerungsprogrammen zugrundeliegende Know-how zu schützen.

Die vorliegende Erfindung wird nun anhand der beigefügten Zeichnung näher erläutert, die einen Datenflussplan gemäß einer Ausführungsform der vorliegenden Erfindung darstellt.

Der Ersteller und Lieferant eines Steuerungsprogramms entwickelt dieses in einer Projektier-Software bzw. Engineeringsystem 1. Der Kunde erhält dieses Steuerungsprogramm über das Internet 2 oder ein beliebiges anderes Netzwerk bzw. andere Verbindung. Der Kunde integriert das empfangene Steuerungsprogramm in sein Engineeringsystem 3 und kann damit seine Zielhardware bzw. sein Runtimesystem 4 ansteuern.

Damit das Steuerungsprogramm bei der Übertragung in öffentlichen Netzen und/oder für den Kunden nicht in allen Details zugänglich ist, wird das Steuerungsprogramm ganz oder teilweise verschlüsselt. Dies kann durch standardisierte Verschlüsselungstechniken, z. B. PGP-Verfahren, erfolgen. Dabei

können symmetrische oder asymmetrische Schlüssel verwendet werden.

Im Einzelnen erstellt der Lieferant zunächst ein unverschlüsseltes Steuerungsprogramm 5 und hält dieses in einer persistenten Datenhaltung 6. Den unverschlüsselten Programmcode 5 bzw. 7 kann der Lieferant aus der persistenten Datenhaltung 6 in einen Programmeditor 8 des Engineeringsystems 1 laden. In dem Editor 8 kann der Lieferant das Programm editieren und zur Verschlüsselung des Programms einen Postprozessor 9 anstoßen, der einen verschlüsselten Programmcode 10 ausgibt. Zur Verschlüsselung verwendet der Postprozessor 9 einen Schlüssel 11. Typischer Weise wird zur Verschlüsselung das standardisierte PGP-Verfahren verwendet. Bei asymmetrischer Verschlüsselung verwendet der Lieferant zur Verschlüsselung einen so genannten „Public-Key" und der Kunde zur Entschlüsselung den dazu passenden „Privat-Key" 12.

Zum Übertragen des verschlüsselten Programmcodes 10 beispielsweise über das Internet 2 werden die Daten zunächst aus der Projektiersoftware 1 exportiert. Vorzugsweise werden die Daten dabei in HTML- bzw. XML-Format oder ein anderes von Standard-Internetclients lesbares Format gewandelt. Der Vorteil derartig formatierter Daten liegt darin, dass mit Standard-Tools auf die Daten zugegriffen werden kann, und der Anwender nicht notwendiger Weise über ein Engineeringsystem verfügen muss.

Nach dem Export werden die verschlüsselten XML-Daten 13 beispielsweise in einem öffentlichen Webserver 14 hinterlegt. Dieser stellt das verschlüsselte Steuerungsprogramm im XML-Format der Allgemeinheit oder entsprechend der Verschlüsselungstechnik nur einen bestimmten, gewünschten Kundenkreis zur Verfügung.

Der Kunde lädt die verschlüsselten XML-Daten 13 in seine persistente Datenhaltung 15. Aus der Datenhaltung 15 werden die

Daten in das Engineeringsystem bzw. die Projektiersoftware 3 des Kunden importiert. Sofern das Engineeringsystem 3 des Kunden nicht auf dem XML-Format oder einem anderen von Standardinternet-Clients lesbaren Format basiert, findet beim Import eine Konvertierung der Daten in das Engineeringsystem-Format statt, wobei der entsprechende, verschlüsselte Programmcode 16 erzeugt wird.

Der Kunde kann nun den verschlüsselten Programmcode 16 in seinem Programmeditor 17, der wiederum Teil des Engineeringsystems 3 ist, beispielsweise zum Parametrieren des zu steuernden Systems, editieren.

Je nach Verschlüsselungstiefe ist der Kunde in der Lage nur die vom Lieferanten gewünschten Daten zu editieren. So ist es möglich, die Daten beliebig tief in horizontaler und vertikaler Richtung zu verschlüsseln.

Eine Verschlüsselung auf einer bestimmten horizontalen Ebene bedeutet, dass beispielsweise Module auf gleicher funktioneller Ebene unterschiedlich verschlüsselt werden. So könnte beispielsweise eine Bibliothek mit den Funktionen a, b, c und d mit mehreren Schlüsselpaaren verschlüsselt werden, so dass die Kunden A, B, C und D nur die jeweils für sie bestimmten Module entschlüsseln bzw. verwenden können.

Das vertikale Verschlüsseln bedeutet ein unterschiedliches Verschlüsseln in verschiedenen hierarchischen, funktionalen Ebenen. So ist es denkbar, dass ein Kunde zum Betreiben des Steuerungsprogramms lediglich die Modulparameter einschließlich der Returnparameter kennen muss. Daher kann der Kopf des Steuerungsprogramms unverschlüsselt bleiben, während der Kern des Programms verschlüsselt ist. Dies dient insbesondere dazu, das der Software zugrundeliegende Know-how zu schützen. Darüber hinaus kann das Softwareprogramm zur Übertragung und Abarbeitung durch den Kunden aber auch komplett verschlüsselt sein und beispielsweise nur für das Servicepersonal vollstän-

dig entschlüsselbar sein. Weitere beliebig granulare Verschlüsselungen sind hier entsprechend dem modularen Aufbau eines Steuerungsprogramms denkbar.

Nach dem Editieren wird das ganz oder teilweise verschlüsselte Steuerungsprogramm in einem Preprozessor 18 des Engineeringsystems 3 entschlüsselt. Hierzu verwendet der Preprozessor 18 den bereits erwähnten privaten Schlüssel 12.

Der vom Preprozessor 18 erhaltene unverschlüsselte Programmcode 19 wird in einem Compiler 20 in einen mikroprozessorspezifischen, ausführbaren Binärcode 21 umgesetzt.

Zur Steuerung eines Systems wird nun der ausführbare Binärcode 21 von der Projektiersoftware bzw. dem Engineeringsystem 3 in die Zielhardware bzw. das Runtimesystem 4 geladen. Dort wird der Binärcode von einem Mikroprozessor abgearbeitet.

Durch die genannte Integration eines Verschlüsselungssystems in Engineeringsysteme unter Verwendung von asymmetrischen Schlüsseln 11, 12 ergeben sich die folgenden Vorteile:

a) Die bekannten Routinen für Ver- und Entschlüsselung wandeln von ASCII-Text in ASCII-Text. Die verschlüsselten Bereiche lassen sich also genauso speichern und transportieren wie die unverschlüsselten Bereiche und bieten damit eine ideale Integration in das weitverbreitete XML-Format. Insbesondere lassen sich zur Weiterverarbeitung der Daten Standard-Tools verwenden.

b) Aufgrund der Verwendung eines Textformats lassen sich auch Teile eines Texts verschlüsseln. Somit kann, wie bereits erwähnt, der Kopf eines Programms mit so genannten Defines zum Anpassen unverschlüsselt bleiben, während der Körper des Programms mit den Funktionen aber geschützt wird.

c) Der Lieferant einer Anwendersoftware, z. B. Compiler oder Projektiertool, gibt dieser ein eigenes Schlüsselpaar. Bei asymmetrischer Verschlüsselung speichert der Lieferant den Public-Key mit den Kundendaten des Anwenders. Damit kann der Lieferant beispielsweise Bibliotheken für bestimmte Kunden mit deren Public-Key verschlüsseln und über beliebige Kanäle an diese Kunden übermitteln. Ein Kopieren der über öffentliche Kanäle zur Verfügung gestellten Anwendersoftware ist in diesem Fall sinnlos, da die Bibliothek ausschließlich auf der Anwendung des vorgesehenen Kunden entschlüsselt werden kann. Auf dieser Basis ist ein Lizenzsystem leicht realisierbar.

d) Die verschlüsselten Texte sind nicht analysierbar. Das interne Know-how bleibt somit geschützt.

e) Durch die Integration einer asymmetrischen Entschlüsselung in einen Preprozessor des Compilers lassen sich Programmteile gegen Missbrauch schützen, ohne den Compiler selbst zu ändern. Der Preprozessor läuft erst bei der Erzeugung des binären Codes für das Zielsystem. Darüber hinaus benötigt auch der Programmeditor keine Änderung, da die verschlüsselten Texte als solche angezeigt werden.

Das oben beschriebene erfindungsgemäße System lässt sich dahingehend abändern, dass das Verschlüsseln direkt in den Exportmechanismus und das Entschlüsseln in den Importmechanismus eingebaut werden. Damit werden dem Kunden allerdings sämtliche Daten des Steuerungsprogramms zum Editieren freigegeben.

Patentansprüche

1. Verfahren zum Transfer von Steuerungsprogrammen durch

Verschlüsseln eines Steuerungsprogrammcodes (5, 7) in einem ersten Entwicklungssystem (1),

Transferieren des verschlüsselten Steuerungsprogrammcodes (10, 16) von dem ersten Entwicklungssystem (1) zu einem zweiten Entwicklungssystem (3), und

Entschlüsseln des verschlüsselten Steuerungsprogrammcodes in dem zweiten Entwicklungssystem (3).

2. Verfahren nach Anspruch 1, wobei das Transferieren ein Exportieren des verschlüsselten Steuerungsprogrammcodes (10, 16) in ein von Standard-Internetclients lesbares Format, insbesondere XML oder HTML, durch das erste Entwicklungssystem (1) und ein Importieren der Daten in dem von Standard-Internetclients lesbaren Format durch das zweite Entwicklungssystem (3) umfasst.

3. Verfahren nach Anspruch 1 oder 2, wobei das Ver- und Entschlüsseln der Daten durch asymmetrische Schlüssel (11, 12) erfolgt.

4. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Verschlüsseln des Steuerungsprogrammcodes nach einem Editieren des Steuerungsprogrammcodes in dem ersten Entwicklungssystem (1) erfolgt.

5. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Entschlüsseln des verschlüsselten Steuerungsprogrammcodes nach einem Editieren des verschlüsselten Steuerungsprogrammcodes in dem zweiten Entwicklungssystem (3) erfolgt.

6. Verfahren nach einem der vorhergehenden Ansprüche, wobei nur ein oder mehrere Teile des Steuerungsprogramms verschlüsselt werden und insbesondere der Kopf des Steuerungsprogramms unverschlüsselt bleibt.

7. Verfahren zur Parametrierung, Projektierung und Inbetriebnahme von Steuerungssystemen und/oder Antrieben durch

Transfer eines Steuerungsprogramms nach einem der Ansprüche 1 bis 6,

Kompilieren des entschlüsselten Steuerungsprogramms und

Abarbeiten des kompilierten Steuerungsprogramms durch einen Mikroprozessor.

8. System zum Transfer von Steuerungsprogrammen mit

einer ersten Entwicklungseinrichtung (1) zum Entwickeln eines Steuerungsprogrammcodes (5, 7), die eine Verschlüsselungseinheit (9) zum Verschlüsseln des Steuerungsprogrammcodes (5, 7) umfasst,

einer Kommunikationseinrichtung (2) zum Transferieren des verschlüsselten Steuerungsprogrammcodes (10, 16) von der ersten Entwicklungseinrichtung (1) zu einer zweiten Entwicklungseinrichtung (3), und

der zweiten Entwicklungseinrichtung (3), die eine Entschlüsselungseinrichtung (18) zum Entschlüsseln des verschlüsselten Steuerungsprogrammcodes (10, 16) umfasst.

9. System nach Anspruch 8, wobei die erste Entwicklungseinrichtung (1) eine Exporteinrichtung zum Exportieren des verschlüsselten Steuerungsprogrammcodes (10, 16) in

einem von Standard-Internetclients lesbaren Format, insbesondere XML oder HTML, und die zweite Entwicklungseinrichtung (3) eine Importeinrichtung zum Importieren der Daten in dem von Standard-Internetclients lesbaren Format umfasst.

10. System nach Anspruch 8 oder 9, wobei das Ver- und Entschlüsseln der Daten durch asymmetrische Schlüssel (11, 12) erfolgt.

11. System nach einem der Ansprüche 8 bis 10, wobei in der ersten Entwicklungseinrichtung (1) ein Postprozessor (9) zum Verschlüsseln des Steuerungsprogrammcodes (5, 7) zwischen einen ersten Editor (8) zum Editieren des Steuerungsprogrammcodes (5, 7) und die Kommunikationseinrichtung (2) geschaltet ist.

12. System nach einem der Ansprüche 8 bis 11, wobei in der zweiten Entwicklungseinrichtung (3) ein zweiter Editor (17) zum Editieren des Steuerungsprogrammcodes (10, 16) zwischen einen Preprozessor (18) zum Entschlüsseln des Steuerungsprogrammcodes (10, 16) und die Kommunikationseinrichtung (2) geschaltet ist.

13. System nach einem der Ansprüche 8 bis 12, wobei nur ein oder mehrere Teile des Steuerungsprogramms (5, 7) verschlüsselt werden und insbesondere der Kopf des Steuerungsprogramms unverschlüsselt bleibt.

14. Anordnung zur Parametrierung, Projektierung und Inbetriebnahme von Steuerungssystemen und/oder Antrieben mit

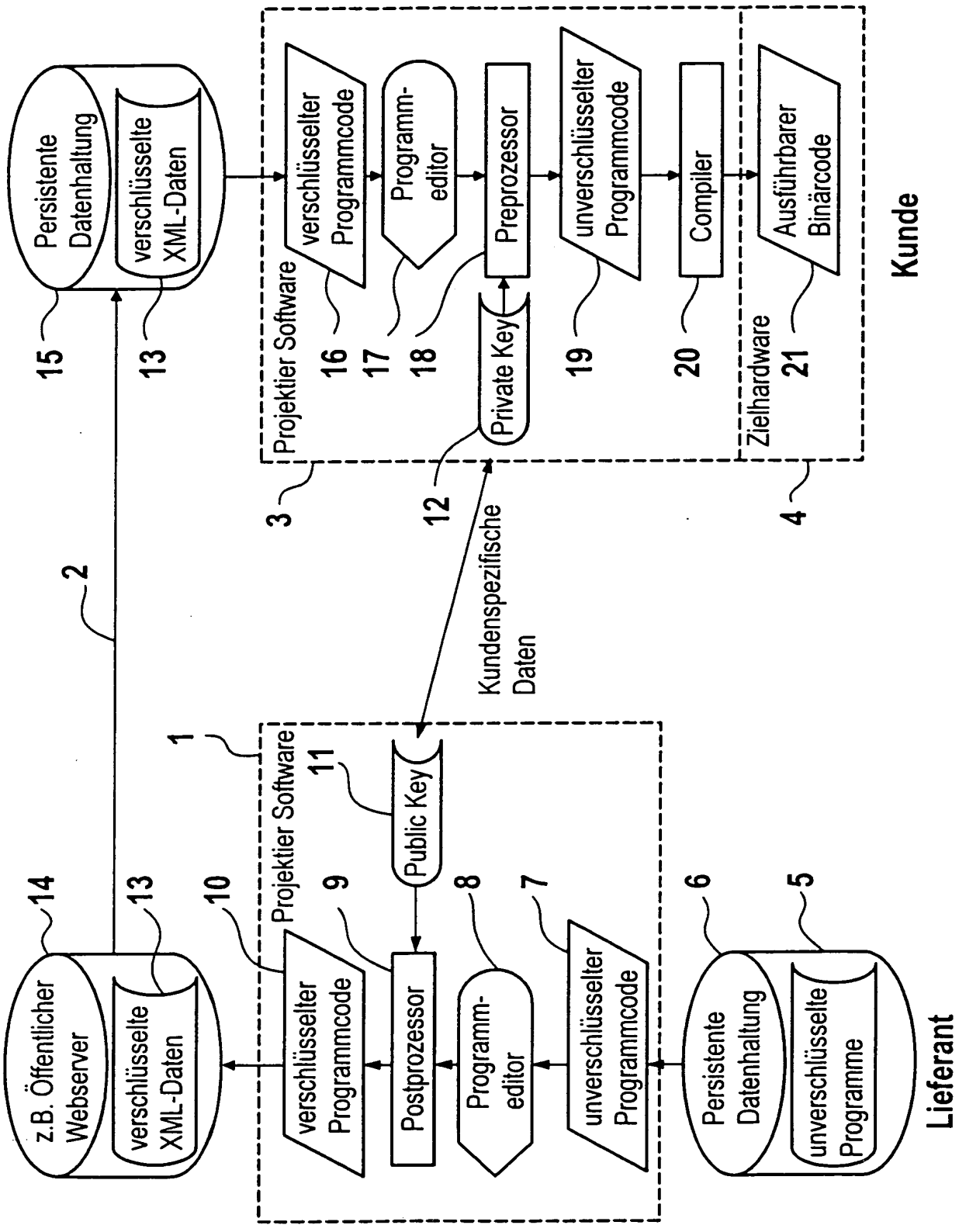
einem System zum Transfer von Steuerungsprogrammen nach einem der Ansprüche 8 bis 13, wobei die zweite Entwicklungseinrichtung (3) einen Compiler (20) zum Kompilieren des entschlüsselten Steuerungsprogramms (19) um-

fasst und einen Mikroprozessor zum Abarbeiten des kompilierten Steuerungsprogramms ansteuert.

Zusammenfassung

Verschlüsselung von Steuerungsprogrammen

Zum Schutz von Steuerungsprogrammen gegen unbefugte Analyse und Benutzung beim Transport über öffentliche Netze werden asymmetrische Schlüssel verwendet. Nach der Erstellung des Steuerungsprogramms im Engineeringsystem (1) des Lieferanten wird das Programm in einem Postprozessor (9) verschlüsselt und in einen öffentlichen Webserver (14) exportiert. Der Kunde lädt das verschlüsselte Programm in seine persistente Datenhaltung (15), importiert es in sein Engineeringsystem (3) und kann es dort zum Parametrieren des Steuerungssystems editieren. Erst nach dem Editieren werden die verschlüsselten Programmteile in einem Preprozessor (18) entschlüsselt und zum Compiler (20) weitergeleitet.


Persistente Datenhaltung
verschlüsselte XML-Daten
15
13
2
Projektier Software
verschlüsselter Programmcode
Programm-editor
Preprozessor
unverschlüsselter Programmcode
Compiler
16
17
18
19
20
Private Key
3
12
Zielhardware
Ausführbarer Binärcode
21
4
Kunde
Kundenspezifische Daten
1
Projektier Software
11
Public Key
z.B. Öffentlicher Webserver
14
13
verschlüsselte XML-Daten
10
verschlüsselter Programmcode
9
Postprozessor
8
Programm-editor
7
unverschlüsselter Programmcode
6
Persistente Datenhaltung
5
unverschlüsselte Programme
Lieferant